WHAT IS CLAIMED IS:

1. A semiconductor device comprising an encryption section which performs at least one of encryption and decryption of a program,

wherein the encryption section includes

an encryption arithmetic processing section capable of executing a plurality of sequences including an encryption process or decryption process of a program, and

an encryption control section for determining whether to permit execution of each of the sequences which can be executed by the encryption arithmetic processing section, and prohibiting the operation of the encryption arithmetic processing section with respect to a sequence whose execution is determined to be impermissible.

2. The semiconductor device according to claim 1, wherein the plurality of sequences include an encryption process or decryption process of a key.

3. The semiconductor device according to claim 1, wherein:

the encryption control section includes a mode ID storage register for storing a mode ID; and

the encryption control section determines whether to permit execution of each of the sequences based on the value of the mode ID stored in the mode ID storage register.

4. The semiconductor device according to claim 3, wherein:

the encryption control section includes a plurality of registers which

correspond to the sequences on a one-to-one basis, each register storing the number of issuances of a corresponding one of the sequences; and

the encryption control section determines whether to permit execution of each sequence while considering the number of issuances of the each sequence which is stored in the corresponding register in addition to the value of the mode ID.

5. The semiconductor device according to claim 3, further comprising a secure memory having an unrewritable area, the unrewritable area storing the mode ID, wherein

the mode ID storage register is writable only at the time of boot-up of the semiconductor device; and

at the time of boot-up of the semiconductor device, the mode ID read from the unrewritable area of the secure memory is written in the mode ID storage register.

6. The semiconductor device according to claim 5, further comprising a boot ROM for storing a boot program, wherein

writing of the mode ID in the mode ID storage register is performed by the boot program stored in the boot ROM.

7. The semiconductor device according to claim 3, further comprising a secure memory for storing an installation mode flag, the installation mode flag indicating whether or not the semiconductor device is booted up for the first time, wherein

the encryption control section determines whether to permit execution of each sequence while referring to the installation mode flag in addition to the value of the mode ID.

8. The semiconductor device according to claim 1, further comprising a boot ROM for storing at least one boot program corresponding to one of the plurality of sequences, wherein

the encryption arithmetic processing section executes the boot program stored in the boot ROM, thereby executing the sequence corresponding to the boot program.

9. The semiconductor device according to claim 1, further comprising a controller for preventing accesses from the outside of the semiconductor device to the registers of the encryption arithmetic processing section and the encryption control section.

10. A semiconductor device comprising an external interface for inputting/outputting a program or data from/to an external memory, the external interface includes

a program processing section for inputting/outputting a program, and

a data processing section for inputting/outputting data,

wherein the program processing section and the data processing section are structured independently from each other.

11. The semiconductor device according to claim 10, wherein the program processing section includes

a through section for inputting/outputting a program as it is, and

a program-decryption cryptography engine for receiving an encrypted program from the external memory, decrypting the encrypted program into a raw (binary) program, and supplying the raw (binary) program to the inside of the semiconductor device.

12. The semiconductor device according to claim 11, wherein:

the through section includes an execution through section and an encryption through section, and

a program input through the encryption through section is executed in the semiconductor device, and a program input through the encryption through section is supplied to and encrypted in an encryption section.

13. The semiconductor device according to claim 12, further comprising an address segment storage register for storing address management information which represents the correspondence between respective areas of the external memory and addresses, wherein

when the semiconductor device accesses the external memory to read a program, the address management information is referred to for determining which of the encryption through section, the execution through section and the program-decryption cryptography engine is activated.

14. The semiconductor device according to claim 13, wherein the address segment storage register is writable only at the time of boot-up of the semiconductor device.

15. The semiconductor device according to claim 14, further comprising a secure memory having an unrewritable area, the unrewritable area storing the address management information, wherein

at the time of boot-up of the semiconductor device, the address management information read from the unrewritable area of the secure memory is written in the address segment storage register.

16. The semiconductor device according to claim 13, further comprising a mode sequencer which has a mode ID storage register for storing a mode ID,

wherein the value of the mode ID stored in the mode ID storage register is additionally considered for determining which of the encryption through section, the execution through section and the program-decryption cryptography engine is activated.

17. The semiconductor device according to claim 16, wherein:

the mode sequencer includes a jumper value determination section; and

a jumper value determined by the jumper value determination section is additionally considered for determining which of the encryption through section, the execution through section and the program-decryption cryptography engine is activated.

18. The semiconductor device according to claim 10, wherein the data processing section includes

a through section for inputting/outputting data as it is, and

a data-encryption/decryption cryptography engine for performing encryption or decryption of data at the time of input/output of the data.

19. A content reproduction method, comprising the steps of:

reading an original content stored in an irreproducible area of an external memory into an LSI device;

generating a data inherent key in the LSI device using an inherent ID stored in an internal memory;

encrypting the original content in the LSI device using the data inherent

key;

storing the encrypted content in a reproducible area of the external memory;

reading the encrypted content stored in the reproducible area into the LSI device;

decrypting the encrypted content in the LSI device using the data inherent key; and

reproducing the decrypted content in the LSI device.

20. The content reproduction method according to claim 19, wherein:

the original content stored in the irreproducible area is a content encrypted with a data common key;

prior to encryption with the data inherent key, the original content is decrypted using the data common key stored in the internal memory.